REMARKS

Claims 1-15 are currently pending in the application with Claims 1, 4, 8, 12 and 14 as independent claims. The Examiner has rejected Claims 14 and 15 under 35 U.S.C. §101 for being directed to non-statutory subject matter. The Examiner rejected Claims 1-6 and 8-13 under 35 U.S.C. §102(e) as being anticipated by Watanabe et al. (U.S. Patent No. 7,072,657). The Examiner further rejected Claims 14 and 15 under 35 U.S.C. §103(a) as being unpatentable over Ueda et al. (U.S. Patent No. 6,289,102) in view of Watanabe.

Reconsideration of the present application is respectfully requested.

Watanabe discloses a method of coordinating the handoff of a mobile carrier between a first access network and a second access network. The method includes attempting a hand-off from a first access network that the mobile carrier is currently operating within to a second access network, wherein the attempting includes authenticating at the hyper operator only that the user may have access to the second access network via a contract earlier established.

Regarding the §101 rejection, the Examiner states that Claims 14 and 15 are not limited to tangible embodiments. The specification has been amended to remove the phrase "and carrier waves." Entry of this amendment is respectfully requested, and is believed to overcome the 35 USC§101 rejection.

Regarding the rejection of independent Claims 1, 4, 8, 12 and 14, under the section "Response to Arguments," the Examiner expressed his disagreement with one of the plurality of arguments presented. In particular, the Examiner stated, at column 6, line 57 through column 7, line 16 and column line 50 through column 9, line 22, Watanabe further teaches that the authentication controller prepares pre-authentication and a shared key. The shared key is computed for each connection and is part of the pre-authentication process for establishment of a VPN between two networks. The Examiner selectively chose to respond to one argument and ignore the other arguments. For example, Applicants argued the following. The Examiner cites

Fig. 7, ref. num 510 and 516 for teaching "differentiating said encryption keys according to a plurality of access authorization types." Reference numerals 510 and 516 depict a "cloud" which typically indicates the "ether" or "public domain" or the medium of propagation of electromagnetic waves. It is unclear how the Examiner makes the inference from the reference numerals to the limitation recited in Claim 1. The Examiner's Response to Arguments is silent regarding above argument.

Furthermore, in an attempt to support his disagreement, the Examiner cites column 6, line 57 through column 7, line 16 and column line 50 through column 9, line 22 as further teaching that the authentication controller prepares pre-authentication and a shared key. It is respectfully submitted, however, that the cited passages, bolster Applicants' argument instead. Column 6, lines 64-65 states, "This shared key is a one-time password to establish a VPN between them." Column 7, lines 4-11 states, "In this scenario, the current access network 502 contacts the H.O.DiC 400 to get the shared key for authentication as well as billing confirmation. For the company intranet 210, the H.O.DiC 400 provides the same shared key that network 502 receives from H.O.DiC 400 to the company intranet 210 for VPN establishment. So, the current access network 502 and the company intranet 210 can authenticate each other via the shared key."(Emphasis added). As can be seen, the shared key is used for authentication. Nowhere in *Watanabe* is it disclosed that the shared key is used for other than authentication. As it is known in the art, authentication is the process of identifying an individual requesting access to a system; it does not necessarily involve encryption and the cited passage of *Watanabe* is silent with respect to encryption. Since the cited prior art supports Applicants' position and the Examiner did not address most of the arguments presented in the last reply, Applicants respectfully resubmit the same arguments to rebut the Examiner's response as articulated above.

With regards to independent Claim 1, the Examiner asserts that *Watanabe et al.* discloses all the elements of the claim. In addition to the arguments above, the Examiner cites col. 7, lines 17-40 for the proposition that "obtaining by at least one wireless station the differentiated encryption keys in advance" reads on *Watanabe et al.* At best, the cited passage discloses that pre-authentication and pre-VPN establishment is possible via the hyper operator distributed center (H.O.DiC). Pre-authentication and pre-VPN establishment will help a fast hand-off. *Watanabe* further discloses since the H.O.DiC has user information, it is possible to have a prearrangement and not to disclose the user's information to the target access network. Clearly, *Watanabe* primary concern is fast hand-off whereas the present invention is directed to access authorization differentiation and secure roaming. Furthermore, all throughout *Watanabe* reference is made to pre-authentication. As it is known in the art, authentication is the process of identifying an individual requesting access to a system; it does not necessarily involve encryption and the cited passage of *Watanabe* is silent with respect to encryption. Accordingly, *Watanabe* fails to anticipate Claim 1.

Therefore, Applicants respectfully submit that the Examiner is incorrect in rejecting Claim 1 of the present invention, as *Watanabe et al.* clearly does not disclose obtaining differentiated encryption keys in advance. This is a clear distinction between the present invention and *Watanabe et al.* Furthermore, Claim 1 has been amended and is further distinguished.

As for independent Claim 4, the Examiner cites col. 7, lines 41-64 for teaching "obtaining an encryption key and updating the shared key set by adding the encryption key to the shared key set in accordance with the determination result of step (c)." As articulated above, authentication is the process of identifying an individual requesting access to a system; it does not necessarily involve encryption and the cited passage of *Watanabe* is silent with respect to encryption. Clearly, *Watanabe* primary concern is fast hand-off whereas the present invention is directed to access authorization differentiation and secure roaming. Accordingly, *Watanabe* fails to anticipate Claim 4.

The Examiner is also incorrect in rejecting Claim 4 of the present invention, as *Watanabe et al.* clearly fails to anticipate Claim 4 and at least does not disclose the above limitation of Claim 4. Furthermore, Claim 4 has been amended and is further distinguished.

As for independent Claim 8, the Examiner cites col. 7, lines 9-16 for teaching "using the selected encryption key to encrypt a transmission message and communicate with the access point not available for communication." Again, authentication does not necessarily involve encryption and the cited passage of *Watanabe* is silent with respect to regarding encryption. Clearly, *Watanabe* primary concern is fast hand-off whereas the present invention is directed to access authorization differentiation and secure roaming. Accordingly, *Watanabe* fails to anticipate Claim 8. Furthermore, Claim 8 has been amended and is further distinguished.

As for independent Claim 12, the Examiner cites col. 7, lines 2-16 for teaching "an encryption key allocation unit which reads an encryption key from the encryption key storing unit corresponding to a determination result of the access authorization determining unit and transfers a value of said encryption key to the wireless station." Again, authentication does not necessarily involve encryption and the cited passage of *Watanabe* is silent with respect to encryption. Clearly, *Watanabe* primary concern is fast hand-off whereas the present invention is directed to access authorization differentiation and secure roaming. Accordingly, *Watanabe* fails to anticipate Claim 12.

Because the above arguments put independent Claims 1, 4, 8, 12 and 14 in condition for allowance, then, at least because of their dependence on these claims respectively, dependent Claims 2-3, 5-10, 9-11, 13 and 15 are also in condition for allowance.

The application as now presented, containing Claims 1-15 are believed to be in condition for allowance. Should the Examiner believe that a telephone conference or personal interview would facilitate resolution of any remaining matters, the Examiner may contact Applicant's attorney at the number given below.

Respectfully submitted,

Paul J. Farrell

Paul J. Farrell
Reg. No. 33,494
Attorney for Applicants

THE FARRELL LAW FIRM, PC
333 Earle Ovington Boulevard, Suite 701
Uniondale, New York 11553
TEL: (516) 228-3565
PJF/EC/